CAPTCHA: Detecting Humans
Gestalt Psychology (1922-1923)

- Max Wertheimer, Wolfgang Köler, Kurt Koffka
- Laws of organization
  - Proximity
    - We tend to group things together that are close together in space
  - Similarity
    - We tend to group things together that are similar
  - Good Continuation
    - We tend to perceive things in good form
  - Closure
    - We tend to make our experience as complete as possible
  - Figure and Ground
    - We tend to organize our perceptions by distinguishing between a figure and a background

Source: http://www.webrenovators.com/psych/GestaltPsychology.htm
Objects on Mars?

Elvis  
Face  
Female statue
HELLO
HELLO
Authenticating humanness

**Battle the Bots**
- Create a test that is easy for humans but extremely difficult for computers

**CAPTCHA:** Completely Automated Public Turing test to tell Computers and Humans Apart
- Image Degradation
  - Exploit our limits in OCR technology
  - Leverages human Gestalt psychology: reconstruction

**Origins**
- 1997: AltaVista – prevent bots from registering URLs with the search engine
- 2000: Yahoo! and Manuel Blum & team at CMU
  - EZ-Gimpy: one of 850 words
- Henry Baird @ CMU & Monica Chew at UCB
  - BaffleText: generates a few words + random non-English words

Source: http://www.sciam.com/print_version.cfm?articleID=00053EA7-B6E8-1F80-B57583414B7F0103
http://tinyurl.com/dg2zf
CAPTCHA Example (2019)

Microsoft

See captchas.net
They had to get more difficult

Advances in character recognition led to automated solving
Problems

• **Accessibility**
  – Visual impairment → audio CAPTCHAs
  – Deaf-blind users are left out
  – Typing text was more tedious on mobile devices

• **Frustration**
  – OCR & computer vision has improved a lot!
  – Challenges that are difficult for computers may be difficult for humans

• **Attacks**
  – Man in the middle attacks
    • Use human labor – CAPTCHA farms
  – Automated CAPTCHA solvers
    • Initially, educated guesses over a small vocabulary
Alternate approaches

- Puzzles, scene recognition
Alternate Approaches

Select 2 objects that are the same shape:

- 7
- A
- P
- m
- s

Verify to continue:

Drag the puzzle piece into place

Create account

Use the arrows to rotate the object to face in the direction of the hand.

1 of 1

Submit

April 29, 2024

CS 419 © 2019-2024 Paul Krzyzanowski
reCAPTCHA

Ask users to translate images of real words & numbers from archival texts
- Human labor fixed up the archives of the New York Times

Two sections

1. known text
2. image text
- Assume that if you get one right then you get the next one correct
  • Try it again on a few other people to ensure identical answers before marking it correct

Google bought reCAPTCHA 2009
- Used free human labor to improve transcription of old books & street data

By 2014:
Google found that AI could crack CAPTCHA & reCAPTCHA images with 99.8% accuracy
NoCAPTCHA reCAPTCHA

Just ask users if they are a robot

• Reputation management
  – “Advanced Risk Analysis backend”
  – Check IP addresses of known bots
  – Check Google cookies from your browser
  – Considers user’s engagement with the CAPTCHA: before, during, and after
    • Mouse movements & acceleration, precise location of clicks

• Latest version: invisible reCAPTCHA
  – Don’t even present a checkbox
NoCAPTCHA fallback

If risk analysis fails,
- Present a CAPTCHA
- For mobile users, present an image identification or labeling problem
Other approaches: Text/email verification

- **Text/email verification**
  - Ask users for a phone # or email address
  - Similar to two-factor authentication but we're not authenticating the user
  - Service sends a message containing a verification code
    - Still susceptible to spamming & automation
    - Makes the process more cumbersome
    - Requires users to disclose some information

- **Measure form completion times**
  - Users take longer than bots to fill out and submit forms
  - Measure completion times
    - Bots can program delays if they realize this is being done
The End